

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A) 平4-1793

⑤ Int. Cl.⁵G 09 C 1/00
G 06 F 15/00

識別記号

3 3 0 A

庁内整理番号

7922-5L
7218-5L

⑬ 公開 平成4年(1992)1月7日

審査請求 未請求 請求項の数 9 (全8頁)

⑭ 発明の名称 暗号化方式及びこれを用いる電子計算機システム

⑯ 特 願 平2-101662

⑰ 出 願 平2(1990)4月19日

⑱ 発 明 者 土 屋 信 東京都大田区下丸子3丁目30番2号 キヤノン株式会社内
 ⑲ 出 願 人 キヤノン株式会社 東京都大田区下丸子3丁目30番2号
 ⑳ 代 理 人 弁理士 大塚 康徳 外1名

明 細 書

1. 発明の名称

暗号化方式及び

これを用いる電子計算機システム

2. 特許請求の範囲

(1) 複数の装置間での使用認可のために伝送されるパスワードの暗号化方式において、

パスワードの入力時固有の情報であつて前記複数の装置で共有できる情報を暗号化鍵として、該パスワードを暗号化することを特徴とする暗号化方式。

(2) 前記パスワードの入力時固有の情報が、発呼時の日付及び／又は時刻情報であることを特徴とする請求項第1項記載の暗号化方式。

(3) 端末装置が通信網を介して電子計算機に接続されている電子計算機システムであつて、

パスワードの入力時固有で電子計算機と共有できる情報を暗号化鍵として該パスワードを暗号化し、前記暗号化されたパスワードを含む発呼時情報を送信する端末装置と、

パスワードの正当性調査時固有で前記端末装置と共有できる情報を暗号化鍵として予め登録されたパスワードを暗号化し、前記端末装置から受信した暗号化されたパスワードとの比較に基づいて、前記端末装置からのアクセスの許可あるいは拒否を決定する電子計算機とを具備することを特徴とする電子計算機システム。

(4) 前記パスワードの入力時固有の情報は発呼時の日付及び／又は時刻情報であり、前記正当性調査時固有の情報は発呼受信時の日付及び／又は時刻情報であることを特徴とする請求項第3項記載の電子計算機システム。

(5) 端末装置が通信網を介して電子計算機に接続されている電子計算機システムであつて、

パスワードの入力時固有の情報を暗号化鍵として該パスワードを暗号化し、前記暗号化鍵及び前記暗号化されたパスワードを含む発呼時情報を送信する端末装置と、

前記端末装置から受信した暗号化鍵に基づいて予め登録されたパスワードを暗号化し、前記端末装置から受信した暗号化鍵の正当性及び暗号化されたパスワードとの比較より、前記発呼時情報が正当であることを調べ、前記端末装置からのアクセスの許可あるいは拒否を決定する電子計算機とを具備することを特徴とする電子計算機システム。

(6) 前記パスワードの入力時固有の情報が、発呼時の日付及び／又は時刻情報であることを

制御手段と、利用者情報が登録されているデータベースとを有することを特徴とする請求項第3項又は第5項記載の電子計算機システム。

特徴とする請求項第5項記載の電子計算機システム。

(7) 前記電子計算機は、前記暗号化鍵の正当性を前記発呼時情報の正当性調査時の日付及び／又は時刻情報に基づいて調査することを特徴とする請求項第6項記載の電子計算機システム。

(8) 前記端末装置は、利用者IDおよびパスワードを入力するための入力手段と、日付や時刻を示す内蔵時計と、プログラムおよびデータを記憶するためのメモリと、該通信網に関する制御を行う通信制御手段とを有することを特徴とする請求項第3項又は第5項記載の電子計算機システム。

(9) 前記電子計算機は、日付や時刻を示す内蔵時計と、プログラムおよびデータを記憶するためのメモリと、該通信網に関する制御を行う通信

3. 発明の詳細な説明

[産業上の利用分野]

本発明は暗号化方式、特に端末装置が任意の情報を発呼信号とともに送信することのできる通信網を介して電子計算機に接続されている電子計算機システムに於る不正利用防止のための暗号化方式及びこれを用いた電子計算機システムに関するものである。

[従来の技術]

従来、利用者が通信網を介して端末装置から電子計算機を利用するときには、利用開始に当たつて利用者IDとパスワードとを電子計算機に送信する。電子計算機側では、受信した利用者IDとパスワードとを電子計算機内のデータベースに格納されている利用者ID及びパスワードと照合して、一致した場合にのみ該端末装置

からの電子計算機の利用を許可する。

この際、端末装置が任意の情報を発呼信号とともに送信することのできる通信網を介して電子計算機と接続されている場合には、端末装置が利用者IDとパスワードとを発呼時情報として送信することができる。すると、通信を確立する前に電子計算機は利用者IDとパスワードとの照合を行い、照合の結果が一致しなかった場合には通信の確立を拒否して該端末装置の電子計算機の利用を拒否できるため、通信網利用料金の節約が図れる。

〔発明が解決しようとしている課題〕

しかしながら、上記従来例では、正規利用者が電子計算機の利用を目的として端末装置から発呼時情報を送信する際に、不正利用を企てる者が通信網上の該発呼時情報を盗むことができれば、

ここで、前記パスワードの入力時固有の情報が、発呼時の日付及び／又は時刻情報である。

又、本発明にかかる電子計算機システムは、端末装置が通信網を介して電子計算機に接続されている電子計算機システムであつて、

パスワードの入力時固有で電子計算機と共有できる情報を暗号化鍵として該パスワードを暗号化し、前記暗号化されたパスワードを含む発呼時情報を送信する端末装置と、パスワードの正当性調査時固有で前記端末装置と共有できる情報を暗号化鍵として予め登録されたパスワードを暗号化し、前記端末装置から受信した暗号化されたパスワードとの比較に基づいて、前記端末装置からのアクセスの許可あるいは拒否を決定する電子計算機とを具備する。

ここで、前記パスワードの入力時固有の情報は

該発呼情報を用いて正規利用者に成り変わつて電子計算機を不正に利用することが可能となる。

これを防止するために正規利用者が頻繁にパスワードを変更することは非常に不便である。

本発明は、上述の問題点に鑑みてなされたもので、発呼時情報を盗むことによる不正利用を防止する暗号化方式及びこれを用いる電子計算機システムを提供する。

〔課題を解決するための手段〕

上述した問題点を解決するために、本発明にかかる暗号化方式は、複数の装置間での使用認可のために伝送されるパスワードの暗号化方式において、

パスワードの入力時固有の情報であつて前記複数の装置で共有できる情報を暗号化鍵として、該パスワードを暗号化する。

発呼時の日付及び／又は時刻情報であり、前記正当性調査時固有の情報は発呼受信時の日付及び／又は時刻情報である。

又、本発明にかかる電子計算機システムは、端末装置が通信網を介して電子計算機に接続されている電子計算機システムであつて、

パスワードの入力時固有の情報を暗号化鍵として該パスワードを暗号化し、前記暗号化鍵及び前記暗号化されたパスワードを含む発呼時情報を送信する端末装置と、前記端末装置から受信した暗号化鍵に基づいて予め登録されたパスワードを暗号化し、前記端末装置から受信した暗号化鍵の正当性及び暗号化されたパスワードとの比較より、前記発呼時情報が正当であるかを調べ、前記端末装置からのアクセスの許可あるいは拒否を決定する電子計算機とを具備する。

ここで、前記パスワードの入力時固有の情報
は、発呼時の日付及び／又は時刻情報である。

又、前記電子計算機は、前記暗号化鍵の正当性
を前記発呼時情報の正当性調査時の日付及び／
又は時刻情報に基づいて調査する。

又、前記端末装置は、利用者IDおよびパス
ワードを入力するための入力手段と、日付や時刻
を示す内蔵時計と、プログラムおよびデータを
記憶するためのメモリと、該通信網に関する制御
を行う通信制御手段とを有する。

又、前記電子計算機は、日付や時刻を示す内蔵
時計と、プログラムおよびデータを記憶するた
めのメモリと、該通信網に関する制御を行う通信
制御手段と、利用者情報が登録されているデータ
ベースとを有する。

〔作用〕

図である。

図中、1は端末装置、2は電子計算機、9は
端末装置1と電子計算機2とを接続する通信網の
ISDNである。端末装置1は、装置全体の制御
を行う演算制御用のCPU3と、CPU3の指示
に従って文字等を表示するCRT表示部4と、
文字入力及び指示用のキーボード5と、現在の
時刻をCPU3に知らせる内蔵時計6と、プロ
グラムおよびデータを記憶するメモリ7と、
CPU3の指示に従いISDN回線9の制御
およびデータ送受信を行い、またISDN回線9
から回線制御信号を受信したときにはCPU3に
知らせる通信制御装置8とを有する。

一方、電子計算機は、装置全体の制御を行う
演算制御用のCPU10と、利用者ID並びに
パスワードなどの利用者情報を格納するデータ

以上のように構成される電子計算機システムに
おいては、電子計算機を利用するための発呼時
には、日付や時刻を暗号化鍵としてパスワードを
暗号化し、該暗号鍵及び／又は該暗号化鍵を用い
て暗号化されたパスワードを含む発呼時情報を
電子計算機に発呼する。電子計算機は、予め登録
されたパスワードを暗号化して、受信した暗号化
されたパスワードと照合し、暗号化鍵をも送る
場合は受信した暗号化鍵すなわち日付や時刻が
現在の日付や時刻と著しく異なるかどうかを検査
した上で、正規利用者であるか否かを判断する。

〔実施例〕

以下、添付図面を参照して本発明の実施例を
説明する。

第1図は本発明の暗号化方式を実現する実施例
の電子計算機システムの概略構成を示すブロック

ベース11と、現在の時刻をCPU10に知らせ
る内蔵時計12と、プログラムおよびデータを
記憶するメモリ13と、CPU10の指示に従い
ISDN回線9の制御およびデータ送受信を行
い、またISDN回線9から回線制御信号を受信
したときにはCPU10に知らせる通信制御装置
14とを有する。

以下、本実施例における電子計算機利用のため
の通信確立までの処理の流れを第2図、第3図の
フローチャートを用いて説明する。第2図は端末
装置1の処理の流れを、第3図は電子計算機2の
処理の流れを示す。

まず、ステップS1において、利用者はキー
ボード5を操作して利用者IDを入力する。入力
された利用者IDはメモリ7に記憶され、同時に
CRT4にも表示される。次に、ステップS2に

において、利用者はキーボード5を操作してパスワードを入力する。入力されたパスワードはメモリ7に記憶される。つづいて、ステップS3において、内蔵時計6より現在の時刻情報を取得する。

ステップS4において、現在の時刻情報を暗号鍵としてパスワードの暗号化を行う。暗号鍵を k 、平文を p としたときの暗号化関数を $f(k, p)$ とする。本実施例において、 k は現在時刻、 p は入力されたパスワードである。メモリ7に記憶されているパスワード p とステップS3において取得した現在時刻 k とから該暗号化関数に従い暗号文 $y = (k, p)$ が計算され、これをメモリ5に記憶する。ステップS5において、メモリ7から利用者ID、暗号化されたパスワード y 、暗号鍵 k を読み出し、通信制御装置8に

たす場合のみ該利用者の利用を許可する。一つでも満たさない条件があれば、該利用者の利用を拒否する。

- (1) 利用者IDがデータベース11に登録されているか(ステップS9)。
- (2) 暗号化鍵 k (端末装置が発呼した時刻)と内蔵時計12から取得した現在の時刻との差が所定時間以内であるか(ステップS10)。
- (3) 受信した暗号化鍵 k とデータベース11に登録されているパスワード p' とから計算した暗号化パスワード $y' = f(k, p')$ が、受信した暗号化パスワード y と一致するか(ステップS11、S12)。

受信した該発呼時情報がこれら3つの条件を満たす場合は、ステップS13で該端末装置との通信を確立するための接続制御信号を送信する。

対しこれらの情報を発呼時情報として電子計算機に発呼するように指示する。通信制御装置8は指示に従い発呼する。

以上、通信の確立までの端末装置1での処理の流れを示したが、次に電子計算機2での処理の流れを第3図を参照しながら説明する。

まず、電子計算機2では、ステップS8において、端末装置1が送信した発呼時情報を受信したかどうかを、通信制御装置14からの信号によりチェックする。受信した場合には、該発呼時情報をメモリ13に記憶し、該利用者の利用を許可するかどうか判断を続くステップS9～S12において行う。すなわち、受信した該発呼時情報に含まれる3つの情報(利用者ID、暗号化されたパスワード、暗号化鍵)に関して、以下に示す3つの条件を満たすかどうかを検査し、すべて満

一方、該発呼時情報がこれら3つの条件を満たさない場合には、利用を拒否する拒否制御信号を該端末装置1に対して送信する。

第2図に戻つて、ステップS6において、端末装置1の通信制御部8が電子計算機2からの制御信号を受信すると、ステップS7において受信した制御信号を判別する。接続制御信号だった場合には、第2図の通信確立の処理を終わつて電子計算機の利用を開始する。拒否制御信号だった場合にはステップS1に戻り、通信確立のための処理を最初からやり直す。

尚、上記実施例では電子計算機が利用者のパスワードそのものをデータベースとして保持しているので、電子計算機の管理者が悪意を持っている場合には不正利用が可能である。そこで、もう一つ暗号化関数 $g(p)$ を導入し、この関数を

用いて暗号化したパスワード $u = g(p)$ をデータベースとして保持する。この場合は、上記実施例における端末装置が発呼時情報として送信する暗号化されたパスワードを $v = f(k, g(p))$ で置き換え、電子計算機が利用者を拒否する条件の(3)を以下の様に置き換える。

(3') 電子計算機が受信した暗号鍵 k とデータベースに登録されている $g(p)$ によつて暗号化されたパスワード u から計算した $v' = f(k, u)$ が、受信した v と異つている。

この変更により、電子計算機管理者は利用者のパスワードを知ることができなくなり、不正利用が不可能になる。

また、電子計算機の利用者拒否条件を追加することによつて、更にセキュリティを向上させることができる。

もパスワードを知ることとはできず、その時点で有効な暗号鍵は時々刻々変わるのでパスワードを知らなければ正しい発呼情報を構成することができないため、不正利用が防止できる。

[発明の効果]

本発明により、発呼時情報を盗むことによる不正利用を防止する暗号化方式及びこれを用いる電子計算機システムを提供できる。

すなわち、発呼時固有の情報、例えば日付や時刻等を暗号化鍵としてパスワードを暗号化することにより、電子計算機の不正利用を試みるものが正規利用者の発呼時情報を盗んだとしても、パスワードを知ることができず、かつその時点で有効な暗号化鍵が刻々と変わるので、電子計算機の不正利用を防止することが可能となる。

4. 図面の簡単な説明

また、本実施例では暗号化鍵である時刻情報を発呼時情報に含んで端末装置より送信する場合のみを説明したが、時刻情報の下位情報(例えば秒の位や分の1位等)を除いて暗号化すれば、電子計算機は自分の内蔵時計の時刻情報による復号化により、暗号化鍵の正当性も同時に調査できる。この場合、復号化したパスワードが他の登録パスワードと同じになる可能性は残るが、時刻情報の情報量やパスワードの工夫により避けることは容易である。

更に、本実施例では時刻情報を暗号鍵としたが、本発明は時々刻々変わる暗号時固有のものであつて、かつ端末装置と電子計算機とで共有できる暗号鍵であれば実現できる。

以上説明した端末装置を用いると、不正利用を試みる者が正規利用者の発呼時情報を盗んだとし

第1図は本実施例の電子計算機システムの概略構成を示すブロック図、

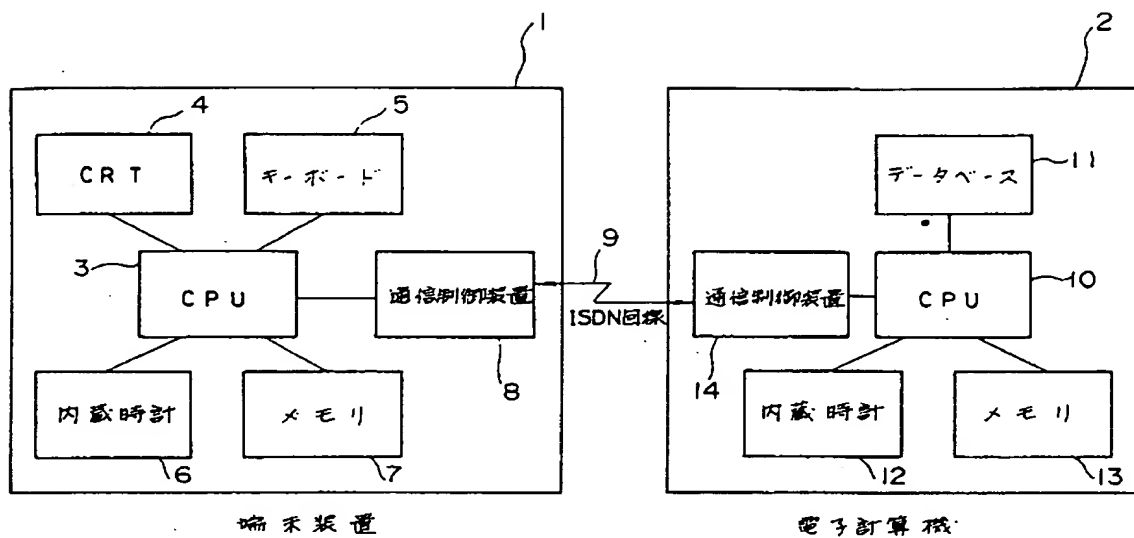
第2図は本実施例の端末装置における電子計算機利用のための通信確立までの手順を示すフローチャート、

第3図は本実施例の電子計算機における電子計算機利用許可までの手順を示すフローチャートである。

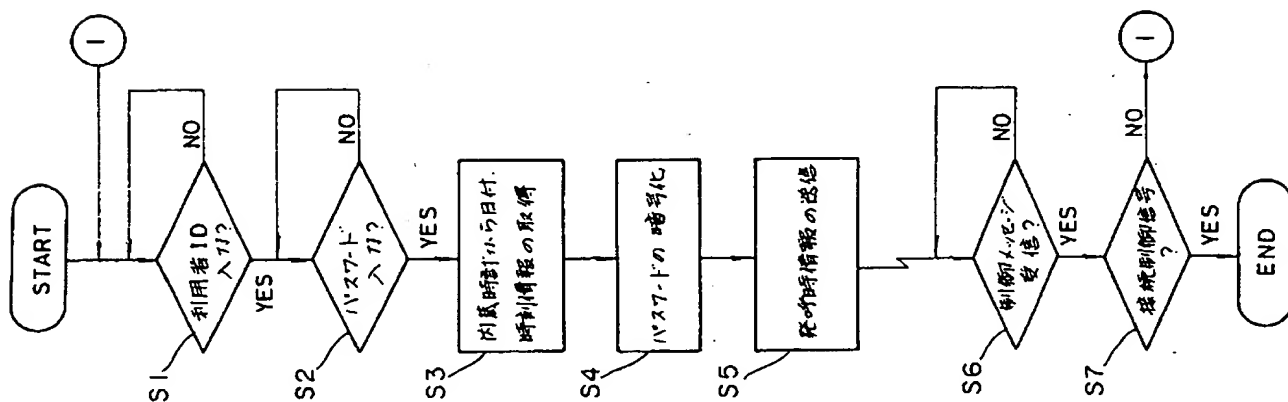
図中、1は端末装置、2は電子計算機、3、10…CPU、4…CRT、5…キーボード、6、12…内蔵時計、7、13…メモリ、8、14…通信制御装置、9…ISDN回線である。

特許出願人 キヤノン株式会社
代理人 弁理士 大塚康徳(他1名)





第 1 図



第 2 図

